تقرير ارتيادي (استراتيجي) سنوي مُحكّم

# ما بعد الإنسانية

## العوالم الافتراضية وأثرها على الإنسان


تحرير

أحمد عمرو

# مقدمة

الحمد لله رب العالمين، والصلاة والسلام على رسول الله، وعلى آله وصحبه أجمعين، وبعد:

تعيش البشرية اليوم على وقع نُقلة بعيدة، تقودها ثورة تكنولوجية هادرة تغلغلت في مسارب الحيـاة الإنسـانية بكافة تنويعاتهـا الاقتصاديـة والاجتماعية والفكرية، سـواء فـي ذلك الفرد والمجتمعات، لم ينجُ مجال تقريبًا من أن يمسه طائف الثورة الرقمية.

الإحصائيات تقول إن هناك أكثر من ٤,٩٦ مليارات مستخدم نشط على الإنترنت في جميع أنحاء العالم وذلك وفقًا لإحصاءات عام ٢٠٢٢، وهذا الرقم يعادل تقريبًا ٦٢٪ من إجمالي سكان العالم.

فـي إحـدى تجلياتها أصبحت العوالم الافتراضية، عالمًا موازيًا لحياتنا الواقعية ويوشـك أن يحـل محلها فتتلاشـى الفواصل بين الواقع والافتراضي. فـي «عالم الميتافيرس» الذي أعلن عنه رئيس شـركة فيسـبوك مارك زوكربيرغ يمكن للموظفين على سبيل المثال العمل في «غرف عمل هورايـزن» (Horizon Workrooms) الجديدة حيث يمكنهم الدخول إلى مكتب عمل افتراضي بشـخصية وهمية «أفاتار» avatar وسيرى المستخدم حاسوبه وزملاءه، ويتفاعل ويتعامل ويتبادل الأفكار معهم بشكل كامل كما لو كان في غرفة عمل حقيقية في مبنى الشركة.

في هذه العوالم الافتراضية اقتصاد جديد قائم على عملات جديدة، والاستثمار في عقارات ومبان وأسـواق افتراضية حيث يمكن شـراء قطع أراضٍ في العديد من عوالم «ميتافيرس» عبر الإنترنـت وتطويرهـا إلـى فنادق ومحال واسـتخدامات أخـرى افتراضية، بهدف زيـادة قيمتها بالعملات المشفرة.

في هذه العوالم الافتراضية من الممكن أن سـتذهب أنت وتبقى شـخصيتك الإلكترونية التي منحتها ذكرياتك وآراءك وحتى حياتك الشخصية بعد مماتك ربما لقرون طويلة.

وهو الأمر الذي يطرح العديد من الأسئلة:

- ما الذي تحمله لنا هذه التكنولوجية الحديثة في طياتها؟

- ما تأثيراتها المستقبلية على واقع المجتمعات حيث ستتلاشى الحواجز بين الدول والكيانات والمجتمعات البشرية؟

- هل نستطيع أن نورث أبناءنا قيمنا وثقافتنا في ظل هذا العالم المنفتح؟

- ما مستقبل عالم الاقتصاد والأعمال في ظل عملات جديدة، حيث مئات الوظائف ستنقرض وأخرى ستظهر حديثا؟

- كيف نستفيد من هذه التكنولوجيا وكيف سنتجنب أضرارها؟

- هل تمثل تلك الثورة التكنولوجية الجديدة مجرد فقاعة سرعان ما تنفجر، أم آن أوان التهيؤ لمعطياتها الجديدة؟

كل تلك الأسئلة وغيرها حاولنا الإجابة عليها من خلال هذا الإصدار التاسع عشر من التقرير الارتيادي والذي هو بعنوان (ما بعد الإنسانية .. العوالم الافتراضية وأثرها على الإنسان). وجاء التقرير لهذا العام في خمسة أبواب مختلفة تناول كلٌّ منها أحد القضايا الفرعية المتعلقة بموضوع تقريرنا، وجاءت موضوعاته على النحو التالي:

حيث تناول **الباب الأول:** النظرية والفكر، والذي يقدم الرؤى النظرية والفكرية المتعلقة بالموضوع الأساس للتقرير، وبدأ الباب بدراسة **(العوالم الافتراضية قراءة مفاهيمية)**

تناولت الدراسة المعاني والمضامين المختلفة لمصطلح العوالم الافتراضية واستعرض الكاتب تاريخ نشأة المصطلح وتطوره وأهم نماذجه وتطبيقاته.

أما الدراسة الثانية **(أشكال المعرفة في ظل العوالم الافتراضية)** فتضمنت أثر تغلغل العوالم الافتراضية في حياتنا وأثرها السلبي على تشكل المعرفة في أذهان الأجيال القادمة وحذر الكاتب من خطورة النشر المشاع في العالم الافتراضي؛ حيث يستطيع المرء أن يكتب ما شاء وكيف شاء، وهو ما يُعرف الآن بذوبان التخصص.

أما **الباب الثاني** وهو الملف الرئيس للتقرير فقد جاء بعنوان **(تكنولوجيا الواقع الافتراضي الآثار والتحديات)** واحتوى على أربع دراسات، الدراسة الأولى كانت بعنوان **(تكنولوجيا نخر**

**الذات.. ظواهر السيلفي والتوثيق نموذجًا)**، تناول الكاتب فيها أثر انتشار ثقافة السليفي على التصورات الأخلاقية والعلاقات الاجتماعية نهيك عن نظرة الإنسان لنفسه وذاته وإعلاء ثقافة الجسد، كما تناولت الدراسة الآثار السلبية لهذه الظاهرة إلى الحد الذي يمكن وصف السيلفي بأنه أحد مظاهر الخلل النفسي.

ثم جاءت الدراسة الثانية **(تماسك المجتمعات في ظل تطورات ما بعد وسائل الاتصال الحديث)** لتسلط الضوء على الصورة التي تنقلها شبكات التواصل الاجتماعية عن الحياة والتي هي في الأخير صورة مشوّهة وغير دقيقة، نظرًا لاعتبارات عدة، أهمها الانتقائية والاجتزاء، وأشارت الدراسة أن انتشار وسائل الاتصال الحديثة كانت له آثارٌ بالغة على تماسك الأسر وانتشار عدد من الظواهر الاجتماعية السلبية التي لم تكن تعرف في مجتمعاتنا إلى وقت قريب.

أما الدارسة الثالثة فجاءت بعنوان **(قراءة في كتاب عالمنا الافتراضي)** والتي استعرضت كتاب: «عالمنا الافتراضي.. ما هو؟ وما علاقته بالواقع؟» لمؤلفه: بيير ليفي، وقام بترجمته عن الفرنسية: رياض الكحال. وأراد الكاتب من هذا المقال تقديم بعض الأفكار للقارئ التي ربما ستكون جديدة ومحفّزة بالنسبة له لفهم أكثر عمقًا لما يعرف الآن بالواقع الافتراضي. وأفكار الكتاب هي نتاج تقاطع التطور التقني الهائل الذي شهدته البشرية في السنوات الأخيرة مع حقول معرفية مختلفة، مثل الفلسفة وعلم الاجتماع والأنثروبولوجيا، ومن هنا تأتي أهمية الكتاب.

الدراسة الرابعة **(تسليع المعلومات الشخصية .. فقدان الخصوصية وأثره على المجتمع)** تناولت الدراسة عددًا من المصطلحات المهمة شكّلت مدخلًا مهمًا لفهم موضوع الدراسة منها الخصوصية الرقمية وإنترنت الأشياء ورأسمالية المراقبة، وأشارت الباحثة أن عمالقة الويب اليوم يتناولون معلوماتنا الشخصية على أنها سعلة يتم تداولها وبيعها، بل صاروا يستخدمون تلك المعلومات في التأثير على أنماط سلوكنا وعادتنا وتصوراتنا أيضًا.

أما **الباب الثالث** في التقرير **(العالم الإسلامي)** فاحتوى على ست دراسات، الدراسة الأولى **(وسائل التواصل الاجتماعي.. المجتمعات البديلة (اللاجئون السوريون نموذجًا)**، ألقت الدراسة الضوءَ على أثر الفضاء الافتراضي في إعطاء مساحة للاجئين في المجتمعات الجديدة ساعدتهم على الاستقرار النسبي بعد حالة التهجير المضاعف التي أبعدوا فيها بالإكراه عن أوطانهم إلا أنها بجانب تلك الجوانب الإيجابية كانت لها جوانب سلبية حيث لعبت دورًا مهمًا في جذب الشباب عبر تلك الوسائل إلى منعرجات منحرفة في بلاد الهجرة سواء أكان انحرافا أخلاقيا أو سلوكيا أو كان تطرفا.

ثانـي تلك الدراسـات (**نظرية المجال العام من الفضاء الواقعي إلى الفضاء الرقمي في العالم الإسلامي**). يصف الكاتب هذا القـرنَ بأنه قرن التقدُّم التكنولوجي بحيث بات يُشار إلى الأشـخاص الذين وُلدوا خلال هذا القرن باسم (السُّكان الأصليين الرَّقميين)، ويُشار إلى الأشخاص الذين يحتاجون إلى التكيُّف مع هذه البيئة باسم (المهاجرين الرَّقميين).

ويـرى أنـه وعلى الرغـم منَ أن التطـوُّرات التكنولوجيَّـة، بطريقة أو بأُخرى، يمكن أن تسـاعد المجتمـع؛ فإنـه لا يزال يبقى على أيـدي الناس لجعل مثل هذه التطوُّرات مفيـدة للمجتمع. ومن هنا يمكن القول إن التطوُّرات التكنولوجيَّة في القرن الحادي والعشـرين تظهر (سـيفًا ذا حدَّين)، يمكن استخدامُه لتحسين المجتمع؛ ومع ذلك يمكن أن تُستخدم -أيضًا- لتدهور المجتمع.

ثـم يأتي **البـاب الرابع (العلاقـات الدولية)** متناولاً أثر وسـائل الاتصـال الحديثة والعوامل الافتراضية على بنية العلاقات الدولية سواء في شقها السياسي أو الاقتصادي.

الدراسـة الأولـى (**مسـتقبل العولمـة الغربيـة وسـيناريوهاتها في ظـل تطـورات العالم الافتراضي**). تناولت الدراسـة أثر ظهور الثورة الرقمية وبروز شـعار القرية الكونية؛ إلى تدشـين الدعـوة إلى العولمـة أو الأمركة، ويرى الكاتب أنها جلبت معها الكوارث الاقتصادية والحروب العرقية والطائفية، وانتشـار الفقر والصراعات في عالم الشـمال، وكذلك انقسـام النظام الدولي إلى عالم الشمال الغني والجنوب الفقير الذي تنهش فيه الرأسمالية المتوحشة.

أما الدراسة الثانية (**مستقبل العلاقات الاقتصادية الدولية مع انتشار العملات الرقمية**)

فتناولت مستقبل العلاقات الاقتصادية الدولية مع انتشار العملات الرقمية وذلك من خلال أربعة محـاور: العملات الرقميـة.. الماهية والتطور وحجم التعاملات، والتحديات التي تواجه هذه العملات والجهـود المبذولـة لمواجهتها، والجوانب الشـرعية لهذه العمـلات، وأثر هذه العملات في مسـتقبل العلاقات الاقتصادية الدولية.

ثـم جـاءت الدراسـة الثالثة: (**أثـر تغلـل التكنولوجيـا بديلاً عـن الإنسـان وأثرها على الاقتصـاد**) وتطـرّق الكاتب فيها إلى المراحـل المختلفة للثورات الصناعية الأولـى والثانية والثالثة، وكيف وصلت البشـرية لمفهوم الثورة الرابعة، التي تسـتند إلى الثورة الرقمية ثم أشـار إلى التخوّفات حول النتائج السلبية لتلك الثورة، وفي مقدمتها: تسبّبها في قدر أكبر من عدم المساواة، لا سيما في قدرتها على تعطيل أسواق العمل، وهو الأمر الذي أكدته العديد من الدراسات والأبحاث، التي أشارت كذلك إلى حتمية التدريب والتطوير ورفع القدرات

كما ألقت الدراسة الرابعة الضوء على ما بات يعرف بالحرب السيبرانية أو الإلكترونية وجاءت الدراسة بعنوان **(الحروب السيبرانية وعلاقات الصراع بين الدول)** ويرى الكاتب أن الهجمات السيبرانية قفزت قفزة كبيرة إلى واجهة الأحداث في السنوات الأخيرة وفرضت نفسها على الواقع والفكر السياسي في ساحة السياسة الدولية والاقتصاد العالمي بسبب تأثيرها البالغ والخطير لكنه يرى أن رغبات الإنسان ونزعاته، سواء كانت في الخير والعدل أو في الشهوات والمال أو التسلية واللهو أو العدوان على الآخرين؛ لم تفادق سجيّتها، فهي في الواقع العملي على الأرض كما في الواقع الافتراضي عبر الفضاء السيبراني.

وفي نهاية الباب جاءت الدراسة الخامسة **(أثر التكنولوجيا الحديثة على بنية الدولة في المستقبل)** لتسلط الضوء على التحديات التي تواجه الدولة في صورتها المعاصرة في التطور التكنولوجي والمعلوماتي الذي خلّفته الثورة الصناعية الرابعة.

أما **الباب الخامس** فقد احتوى على دراستين، أولهما كانت بعنوان **(الكيانات الدعوية وآليات الاستفادة من تطورات وسائل الاتصال).** وسعت الدراسة إلى إظهار دور وسائل التواصل في ذلك، حيث كان لها النصيب الأكبر في إحداث فوضى عارمة في المجتمعات المسلمة خاصة، وتناولت الدراسة واقع وحال الكيانات الدعوية، المنوط بها مواجهة هذه الأخطار والتهديدات، وبيان بعض أدوارها ومهامها، وواجب العلماء، والدعاة، والمصلحين، والولاة المخلصين، وجميع المؤسسات المجتمعية.

وأخيرًا كانت دراسة **(التربية ... في ظل تكنولوجيا خارج السيطرة)** التي تناولت الأزمة التربوية والتي ارتبطت بالتقنية واستخدام الأجهزة الإلكترونية، نتيجة زيادة معدل استخدام الأجهزة والتقنية الحديثة، وهذه قريبة بالناحية الطبية والسلوكية. إضافة إلى القضية الأخطر والأهم وهي المحتوى المعروض على أبنائنا والأجيال القادمة، وما يحويه من قيم وثقافات متصادمة مع عقيدتنا وأخلاقنا، وتطرقت الدراسة إلى وسائل حماية الأبناء من ذلك الطوفان التقني، منها: ترك قنوات حوار بيننا وبينهم نحاول فيها إصلاح ما تم إفساده وإبقاء رصيد الفطرة الطيبة محفوظاً داخلهم دون خسائر كبيرة.

# الفهرس

# الحرب السيبرانية والصراع بين الدول

عبد المنعم منيب

## مستخلص

تُعـرف الحرب السـيبرانية بأنها قيام دولـة أو فواعل من غير الدول بشـنّ هجوم إلكتروني يمثّل أعمالاً عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية، واقتصادية، وإجرامية، وغيرها.

والهجمات السيبرانية هذه باتت تهدّد الأمن القومي للدول؛ بسبب أن المصالح القومية للدول في الفضاء السيبراني أو الإلكتروني قد تعاظمت بعد زيادة اعتماد الدول على ربط البنى التحتية لهـا بالفضـاء السـيبراني في بيئة عمل متشـابكة، وهي ما يطلـق عليه «البنيـة التحتية القومية للمعلومـات» (NII)، مثل: قطاعات الطاقـة، والاتصالات، والنقل، والخدمـات الحكومية والمالية والتجارة الإلكترونية، فضلاً عن المؤسسـات العسـكرية والأمنية، وغيرهـا. ومن هنا، فأي تهديد لأحد هذه الأهداف أو كلها يمثل إضراراً للأمن القومي للدولة.

ومن هنا، نجد أن رغبات الإنسـان ونزعاته، سـواء كانت في الخير والعدل أو في الشـهوات والمـال أو التسـلية واللهـو أو العدوان علـى الآخرين؛ هي نفسـها، وهي في الواقـع العملي على الأرض كما في الواقع الافتراضي عبر الفضاء السـيبراني؛ فالنوازع والرغبات تنتشـر في الواقع السيبراني، وسيزداد وجودها كلما زادت قدرة الإنسان على استخدام هذا الفضاء السيبراني. وفي قلب ذلك كله يأتي الصراع والحرب والهجمات السيبرانية المتعددة بكل أنواعها، ولا يظن أحد أن التقدم العلمي قد يقيّد رغبات ونوازع الإنسان أو يغلب عليها طابع العقل والمنطق، فالأمر كما قال كلاوزفيتز عن طبيعة الحرب: «من الممكن أن يجرف الحقد الشرس أكثر الأمم تمدّناً وتحضراً».

وإن كان الأمر كذلك، فيمكننا القول إن الإنترنت ووسـائل الحرب السـيبرانية وفرت فرصة للمسـتضعفين والمظلومين للانتصاف بدرجة أو أخرى من ظالميهم ومسـتضعفيهم، عبر استخدام الهجمات والحروب السـيبرانية؛ بسبب انخفاض تكلفتها والسـهولة النسبية لاستخدامها وفرص

الإفلات منها دون خسائر أو بخسائر محدودة، كما رأينا في الهجمة السيبرانية الأخيرة على الصين التي نتج عنها أخذ نسخة من مستندات الشرطة الصينية في مكان احتجاز وتعذيب الملايين من أقلية الإيغور الصينية المسلمة ونشرها على الرأي العام العالمي وفضح جمهورية الصين، ما تسبّب في الضغط عليها سياسياً ومعنوياً، ومن جانب آخر شكّلت ثغرة واسعة أمام كل ناعق يريد أن يهدّد أمن دولنا، خاصة أننا أمام تلك الهجمات الإلكترونية لا نمتلك التكنولوجيا المتقدمة التي تتيح لنا صدّ هكذا هجمات.

# الحرب السيبرانية والصراع بين الدول

عبد المنعم منيب

## مقدِّمة

قفزت الهجمات السيبرانية إلى واجهة الأحداث في السنوات الأخيرة وفرضت نفسها على الواقع والفكر السياسي في ساحة السياسة الدولية والاقتصاد العالمي، بسبب تأثيرها البالغ والخطير. فهل تؤدي هذه الهجمات السيبرانية إلى اندلاع حروب سيبرانية أو عسكرية إقليمية أو دولية واسعة النطاق؟ وهل تشجع الحروب السيبرانية على إلهاب الصراع الدولي وتغذي العدوانية عند العديد من القوى الدولية والإقليمية، ما قد يسحب القوى المتصارعة للانزلاق إلى حرب باردة أو حرب ساخنة تقليدية؟ أم هل تصير إحدى أدوات الحرب الباردة أو الحرب الساخنة، سواء كانت تقليدية أو هجينة، وتحكمها نفس قوانينها الدولية والأعراف السائدة في حالات الصراع الدولي والإقليمي؟

كل هذه أسئلة فرضها الواقع السيبراني المعاصر وما صحبه من فرص ومخاطر. ويحاول هذا البحث الإجابة عنها بوضوح واختصار عبر الصفحات التالية.

وسوف نعتمد في هذا البحث على المنهج التاريخي، إلى جانب المنهج المقارن، لإجراء التحليل حول الحروب السيبرانية المعاصرة والقضايا المتصلة بها، بجانب الاتكاء على المنهج الوصفي في بعض القضايا.

### التعريف بالحرب السيبرانية

للتعرف إلى ماهية الحرب السيبرانية (Cyber War) يجب أن نشير إلى معنى الحرب وأهدافها وأن نفرّق بين أنواع الحروب وأجيالها المتعددة. إن جوهر الحرب يدور حول إكراه الخصم على تنفيذ إرادتنا، وذلك عبر أعمال القوة والعنف[١]. ولا شك في أن الهدف الأول للحرب هو هدفها

(١) راجع: كارل فون كلاوزفيتز، الوجيز في الحرب، ترجمة أكرم ديري والهيثم الأيوبي، ط المؤسسة العربية للدراسات والنشر، بيروت ١٩٨٨، الطبعة الثانية، ص ٧٤ وما بعدها.. وأيضاً: كارل فون كلاوزفيتز، عن الحرب، ترجمة سليم شاكر الإمامي، ط المؤسسة العربية للدراسات والنشر، بيروت ١٩٩٧، الطبعة الأولى، ص ١٠٣ وما بعدها.

السياسي[١]، والذي عادة ما يتحقّق بإخضاع إرادة العدو، هذه الإرادة التي تتولى الحرب إخضاعها عبر تحطيم الطاقات المادية والمعنوية للعدو المستهدف؛ فالطاقات المادية تتحطم في المعارك الحربية، أما الطاقات المعنوية فتتحطّم عبر حرب نفسية تستكمل معارك الميدان الحربي[٢]، ومن ثم تجبر الحرب هذا العدو على الاستسلام والخضوع لإرادة المنتصر، وكما يقول كارل فون كلاوزفيتز- محقاً: «الحرب ليست من عمل السياسة فقط، بل إنها أداة سياسية حقيقية، إنها استمرار للنشاط السياسي بوسائل أخرى»[٣].

إن الإخضاع الكامل لإرادة العدو ربما كان ممكناً حتى منتصف القرن العشرين الميلادي، لكن ولادة الرادع النووي والأسلحة فائقة التدمير والعديد من الاستراتيجيات العسكرية الجديدة كالحرب غير المتماثلة[٤] (Asymmetric Warfare)؛ كلها عزّزت الردع المتبادل، ما جعل هذا الإخضاع الكامل لإرادة العدو أمراً شبه مستحيل[٥]، وهذا حدا ببعض المنظّرين الاستراتيجيين إلى اقتراح تعريف آخر لهدف الصراع، وهو: «تصادم إرادات وقوى خصمين أو أكثر يكون فيه هدف كل طرف من الأطراف تليين إرادة الآخر حتى ينتهي الصراع بما يحقق الأهداف والأغراض الرئيسية للأطراف المتصارعة»[٦]، فصار الأمر «تليين إرادة الخصم» بدلاً من «إخضاع إرادته إخضاعاً كاملاً».

**تعرف الحرب السيبرانية بأنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثّل أعمالاً عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية، واقتصادية، وإجرامية، وغيرها.**

إن الحرب الحديثة شهدت أطواراً عدة – وسموا كل طور منها جيلاً – بدءاً باستخدام «القوة البشرية المكثفة» كجيل أول، إلى استخدام «قوة النيران» كجيل ثانٍ، ثم استخدام «المناورات» في الجيل الثالث من الحرب، وتجلت في الحرب العالمية الثانية، خاصة من قبل ألمانيا، وأخيراً جاء ما سمي بحروب الجيل الرابع القائمة على استخدام «توليفة من الأدوات السياسية والاقتصادية والاجتماعية والنفسية» لتحقيق أهداف الحرب[٧]. وبالمواكبة

(١) راجع: كارل فون كلاوزفيتز، عن الحرب، م.س.ذ، ص ٨٠٠ وما بعدها.

(٢) راجع: محمود شيت خطاب، إرادة القتال في الجهاد الإسلامي، ط دار الفكر، القاهرة ١٩٧٣، الطبعة الثانية، ص ٢٦.

(٣) كارل فون كلاوزفيتز، عن الحرب، م.س.ذ، ص ١٢١.

(٤) لمزيد من التفصيل عن الحرب غير المتماثلة انظر: ضياء الدين زاهر، رؤية مستقبلية: الحروب غير المتكافئة: الجيل الرابع وما بعده، مجلة السياسة الدولية، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة ٢٧ نوفمبر ٢٠١٤، على الرابط التالي: **https://cutt.us/mOIDb**، تاريخ المشاهدة ٢٧ مايو ٢٠٢٢.

(٥) ولنتأمل هزيمة الولايات المتحدة وانسحابها من فيتنام وهزيمة الاتحاد السوفيتي وانسحابه من أفغانستان، وأخيراً هزيمة الولايات المتحدة وانسحابها من أفغانستان، وعجز إسرائيل عن اقتحام غزة عدة مرات في سنوات عدة، وذلك كله على سبيل المثال لا الحصر.

(٦) انظر: أمين هويدي، الأمن العربي المستباح، دار الموقف العربي، القاهرة، بدون تاريخ، ص ١٤.

(٧) انظر: شريف عبد الرحمن، حروب الجيل الرابع بين الرواية الأمريكية والرواية المصرية، ط دار البشير، الطبعة الأولى، القاهرة ٢٠١٦، ص١٦.. وانظر شرح مفصل ومطول من منظور آخر في: إميل خوري، صراعات الجيل الخامس، ط شركة المطبوعات للتوزيع والنشر، بيروت، الطبعة الأولى ٢٠١٦، ص ٢٩ وما بعدها.

مع هذا الجيل الرابع من الحرب، ظهر ما أطلق عليه الحرب السيبرانية (Cyber war)، وهي حرب وُلدت من رحم التحولات المتسارعة الناتجة عن الثورة العلمية والصناعية في مجال الحاسوب (Computer) والتطبيقات الرقمية (Applications) والإنترنت (Internet) ثم إنترنت الأشياء (IoT)[١]، فما هي الحرب السيبرانية؟

تعرف الحرب السيبرانية بأنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثّل أعمالاً عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية، واقتصادية، وإجرامية، وغيرها[٢].

والهجمات السيبرانية هذه باتت تهدّد الأمن القومي للدول، بسبب أن المصالح القومية للدول في الفضاء السيبراني أو الإلكتروني قد تعاظمت بعد زيادة اعتماد الدول على ربط البنى التحتية لها بالفضاء السيبراني في بيئة عمل متشابكة، وهي ما يطلق عليه «البنية التحتية القومية للمعلومات» (NII)، مثل: قطاعات الطاقة، والاتصالات، والنقل، والخدمات الحكومية والمالية والتجارة الإلكترونية، فضلاً عن المؤسسات العسكرية والأمنية، وغيرها. ومن هنا، فأي تهديد لأحد هذه الأهداف أو كلها يمثل إضراراً للأمن القومي للدولة.

**والهجمات السيبرانية متعدّدة في نوعها، مثل[٣]:**

- **إتلاف المعلومات أو تعديلها**: حيث الوصول إلى المعلومات المستهدفة وإتلافها أو تعديلها دون أن يظهر ذلك لأصحابها، ما قد يؤدي إلى كارثة عند استخدامها دون اكتشاف ما طرأ عليها.

- **التجسس وجمع المعلومات** عن الخصم دون تدميرها ولا تغييرها، وتكون المعلومات المستهدفة عادة سرية عسكرية أو اقتصادية أو سياسية أو صناعية وتقنية.

- **تدمير أو تعطيل** منشأة أو مؤسسة ما أو سدود المياه أو محطات كهرباء أو وقود ونحوها، عن العمل عبر تعطيل أو إتلاف نظم الحوسبة التي تشغلها أو تتحكم فيها.

---

(١) إنترنت الأشياء (**Internet Of Things**) هو اتصال مختلف الأجهزة المادية بشبكة الإنترنت وقدرة كلّ جهاز على التعريف بنفسه للأجهزة الأخرى، فهي شبكة افتراضية تجمع بين مختلف الأشياء المصنفة ضمن الإلكترونيات، البرمجيات، أجهزة الاستشعار، المحرّكات، وتصل بينها عن طريق الإنترنت، ما يتيح لهذه الأشياء إمكانية تبادل البيانات فيما بينها. وهو لا يقتصر على الجمادات والأجهزة الصغيرة وحسب، فقد يكون «الشيء» شخصاً يحمل معه جهازاً لمراقبة نبضات القلب مثلاً، أو طفلاً يحمل جهاز تتبع، أو سيارة مزودة بأجهزة استشعار أو أنظمة الإضاءة في المنازل ومراكز التسوّق أو ماكينات البيع وغيرها، فهو يشمل كل شيء قد يخطر على البال، لمزيد من التفاصيل انظر: بدون كاتب، «تعرف على تخصصات إنترنت الأشياء وأشهر وظائفه ومجالاته»، على الرابط التالي: **https://cutt.us/oVqnA**، تاريخ المشاهدة ٢٩ مايو ٢٠٢٢.

(٢) رغم ذيوع مسمى «الحرب الإلكترونية» إعلامياً، فإنه يعد مصطلحاً قديماً كان بالأساس مقصوراً على رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، بينما الواقع الراهن في الفضاء الإلكتروني أصبح يشمل شبكات الاتصال والمعلومات والبنية التحتية لكافة الخدمات والمؤسسات المدنية والعسكرية، وانظر: عادل عبد الصادق، أنماط «الحرب السيبرانية» وتداعياتها على الأمن العالمي، مجلة السياسة الدولية، م.س.ذ، ١٤ مايو ٢٠١٥، على الرابط التالي: **https://cutt.us/KOLIW**، تاريخ المشاهدة ٢٨ مايو ٢٠٢٢.. ويلاحظ أن دليل الأمم المتحدة الصادر عام ٢٠١٧ بشأن الهجمات السيبرانية قد عرفها بأنها "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها»، انظر: صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير في العلوم السياسية غير منشورة، كلية الآداب والعلوم جامعة الشرق الأوسط، عَمَّان، يوليو ٢٠٢١ ، ص ٦٩.

(٣) إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، في مجلة العلوم القانونية والسياسية، الجزائر، ج١٠ العدد ١، ص ١٠٢٣.

- **ارتهان آلاف الأجهزة والشبكات أو تعطيلها** بهدف الحصول على فدية لإطلاق سراحها.

- **الحصول على معلومات أو تحريف معلومات أو تسريب معلومات** ومن ثم نشرها من أجل التأثير في مجريات الأحداث، مثل اختراق البريد الإلكتروني لهيلاري كلينتون ونشر محتوياته للتأثير في الانتخابات الرئاسية لصالح المرشح الرئاسي حينئذ دونالد ترامب عام ٢٠١٦.

وعادة ما تستخدم الهجمات السيبرانية برمجيات خبيثة تهاجم أنظمة التحكم للمنشآت، كمحطات الطاقة وأنظمة السكك الحديدية، أو تستخدم برمجيات معدّة لاختراق أنظمة البنوك وتعطّل آلاف العمليات المالية التي قد تسبّب خسائر ضخمة للشركات والأفراد، أو تحوّل مليارات الأموال لحسابات سرية.

**والفاعلون في مجال الحرب السيبرانية متعدّدون، فبالإضافة إلى الدول التي لديها قدرة على تنفيذ هجمات سيبرانية متعددة، هناك الفاعلون من غير الدول، وهم أنواع عدة، مثل:**

- **الأفراد:** الذين يمتلكون معرفة تقنية عالية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم ومن ثم ملاحقتهم.

- **الشركات متعددة الجنسيات:** حيث تمتلك كبريات شركات التكنولوجية قدرات سيبرانية تفوق العديد من الدول، مثل شركات جوجل وفيس بوك وميكروسوفت وآبل وأمازون، ومن أمثلة قدرات هذه الشركات الأزمة التي حدثت بين جوجل والصين بسبب المحتوى، وكذلك تسريب الفيس بوك بيانات المستخدمين لصالح شركة «كامبريدج أناليتيكا» التي استعانت بها لصالح حملة انتخاب الرئيس الأمريكي ترامب.

- **المنظمات الإجرامية:** حيث تقوم هذه المنظمات بالعديد من الهجمات السيبرانية بهدف سرقة المعلومات أو الأموال أو الابتزاز، بهدف الحصول على الأموال أيضاً، وهذه تقدر قيمتها بمئات المليارات من الدولارات سنوياً.

- **الجماعات والمجموعات غير الحكومية:** وهذه متعددة الاتجاهات ومختلفة الأهداف، ولعل أبرز المجموعات التي مارست عملاً سيبرانياً مؤثراً في الواقع الدولي، هي المجموعة التي نشرت ملايين الوثائق السرية الأمريكية المعروفة بـ «Wikileaks».

وسبب خطورة هذا النوع من الحرب هو أن العالم أصبح كأنه قرية واحدة بفعل ربطه بوسائل المواصلات والاتصالات، ومن ذلك شبكة الإنترنت التي تنقل الصوت والصورة والمعلومات من أي مكان في العالم لأي مكان آخر في لمح البصر. كما أصبحت أغلب البرمجيات اللازمة للتعامل مع كل هذه الشبكة بكل تفريعاتها متوفرة اليوم بشكل مفتوح، فكثير منها متاح للجميع (Open Source)، وصار استخدام البرمجيات واستخدام شبكة الإنترنت متاحاً بكل سهولة للأفراد ذوي المعرفة ويتيح لهم

قــدرات وفرصــاً وإمكانات لم تكــن متاحة من قبل غيــر لحكومات الدول المتوســطة والكبرى، وفتحــت هذه المعارف الباب على مصراعيه لكل مــن يرغب في تطوير أنظمــة برمجية تحقق له أهدافه دون الحاجة لاستثمارات كبيرة.

كمــا صــارت أغلــب – إن لــم يكــن كل – المنشآت والمؤسسات العسكرية والمدنية والهياكل الإداريــة الحكومية وغيــر الحكومية، تعمل عبر أنظمــة تحكم حاســوبية مرتبطــة بشــكل أو بآخر بشــبكة الإنترنت، ويمكن لأي شــخص مؤهل جيداً فــي مجــال البرمجيــات وأمن الشبكات، أن يخترق هذه الأنظمة فيعطل هذه المنشــأة أو المؤسســة أو يخربهــا بدرجات متفاوتة بحســب درجــة مهارته وهو جالــس على مكتبه دون أن يتحــرك مــن مكانه، وحدث هــذا كثيراً في الســنوات القليلة الماضية من قبل أفراد تارة ومن قبل دول تارة أخرى[١]. كما أن هناك تقنيات الطائــرات دون طيار التي تعتمد في عملها على التكنولوجيا الحاســوبية، والذي يعنينا منها في هــذا البحث هــو إمكانات اســتخدامها لإجراء اختــراق إلكترونــي لأنظمــة إلكترونيــة تشــغل نظاماً للعدو المســتهدف، سواء كان نظاماً لموقع أو منشــأة مدنيــة أو عســكرية، إذ يمكــن لهذه الطائــرات الوصــول لهذه الأهــداف وإمطارها بحزمــة من المعلومات التي تهــدف إلى تعطيلها أو التحكــم فيهــا، وهناك العديد مــن التجارب التي تجريها الدول المتقدمة للتجهيز لاســتخدام هذه التقنيات القائمة على تكنولوجيا الحوســبة والــذكاء الصناعــي وإنترنــت الأشــياء لتدمير أهــداف عســكرية أو مدنية، ســواء كانت هذه الأهداف جوية أو بحرية أو برية[٢].

**عــادة مــا تســتخدم الهجمــات الســيبرانية برمجيــات خبيثة تهاجم أنظمة التحكم للمنشآت، كمحطات الطاقــة وأنظمــة الســكك الحديدية، أو تســتخدم برمجيات معدّة لاختراق أنظمة البنوك وتعطّل آلاف العمليات المالية التي قد تسبّب خسائر ضخمة.**

**ويمكــن تصنيــف الحرب الســيبرانية وفق أنماط عدة، هي[٣]:**

**الأول - الحــرب الســيبرانية منخفضــة الشــدة:** عبــر اســتخدام الفضــاء الإلكترونــي لصراع منخفض الشــدة، ويكــون بــارداً، أي غيــر مصحــوب بعمليات عســكرية تقليديــة، كما أنه لا يســتهدف الهيمنة الكاملــة على قوى الخصم أو تدميرهــا كلها، فهو جزئــي أكثر من أن يكون شــاملاً أو واســع المجال في أهدافــه، وعادة ما يعبّر عن صراع مستمر بين الفاعلين المتنازعين، وقــد يمتد لفترات طويلة، كما أنه عميق الجذور ويشمل مجالات متعددة: ثقافية، أو اقتصادية، أو اجتماعيــة. والمعتاد أن يعتمد على القوة الناعمة

---

(١) انظر: إميل خوري، م.س.ذ، ص ٢١٥ وما بعدها.

(٢) انظر: إميل خوري، م.س.ذ، ص ٢٢٠ وما بعدها. وقد ذكر المؤلف العديد من الأمثلة المهمة التي طبقت عليها التجارب والتدريبات العملية فليراجعها من يرغب في مزيد من التفاصيل.

(٣) باختصار وزيادات نقلاً عن: عادل عبد الصادق، م.س.ذ.

للحروب السيبرانية وليس شرطاً أن يتطور إلى استخدام القوة المسلحة بشكلها التقليدي.

ولهذه الحرب السيبرانية الباردة وسائل عدة، منها: الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وحرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية.

وفي هذا النمط من الحرب السيبرانية تنشط مجموعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية، مثل جماعة «ويكيليكس» (Wikileaks)، و«أنونيموس» (Anonymous)، كما قد تنشط مثل هذه المجموعات أيضاً في حالات الأزمات الدولية، مثل التوتر بين أستونيا وروسيا في عام ٢٠٠٧، وكذا الهجمات السيبرانية المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين إيران وإسرائيل والولايات المتحدة، وأخيراً ما حدث في الحرب الروسية - الأوكرانية.

**الثاني - الحرب السيبرانية متوسطة الشدة:** وفيها يكون الصراع السيبراني بمنزلة أداة موازية لحرب تقليدية دائرة على الأرض، ويعبر ذلك عن حدة الصراع بين الأطراف، كما قد يساند العمل عسكرياً، وفيه تدور حروب الفضاء الإلكتروني عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشنّ حرب نفسية ضد الخصوم، وغيرها.

وتاريخياً، تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو في عام ١٩٩٩ على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات اتصالات للخصوم، كما برزت خلال الحرب بين حزب الله وإسرائيل ٢٠٠٦، وبين روسيا وجورجيا ٢٠٠٨، والمواجهات بين حماس وإسرائيل ٢٠٠٨ و٢٠١٢.

**الثالث - الحرب السيبرانية الساخنة مرتفعة الشدة:** وهي حرب سيبرانية منفردة وغير مصحوبة بأعمال عسكرية تقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كان احتمال حدوثها وارد في المستقبل مع تطور القدرات التكنولوجية.

وهذا النمط من الحرب السيبرانية يسيطر عليه البُعد التكنولوجي، فتستخدم الأسلحة السيبرانية فقط ضد منشآت العدو، مع اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بُعد، مع توفر القدرات التقنية في الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية.

ولذلك كله تستخدم القوى الدولية الكبرى حالياً الفضاء الإلكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة أولى لحواسيب العدو، واختراق العمليات العسكرية للخصوم سيبرانيّاً، أو حتى استهداف الحياة المدنية، والبنية التحتية المعلوماتية، والهدف من وراء ذلك تحقيق «هيمنة إلكترونية واسعة» بشكل أسرع في حالة نشوب صراع.

لا سيما وأنه قد شهدت الأسلحة الإلكترونية تطوراً أكبر في قدرتها على التأثير في الخصوم،

مثل أسلحة الميكروويف عالية القدرة، والهجمات الإلكترونية عبر الفيروسات، وغيرها من أساليب الاعتداء السيبراني.

**وانطلاقاً من هذا الواقع السيبراني الجديد، فقد برزت في فضاء الفكر السياسي والاستراتيجي مفاهيم عدة مرتبطة بطبيعة واقع الحرب السيبرانية وهجماتها، ومن أبرز هذه المفاهيم نجد المفاهيم التالية:**

**الأمن السيبراني:** صار مصطلح الأمن السيبراني يستخدم لتلخيص السياسات العامة والتدابير الأمنية والمبادئ التوجيهية وطرق إدارة المخاطر والحماية والتدريب ومختلف التقنيات والأدلة التي يمكن استخدامها والاعتماد عليها لحماية أجهزة الحاسوب وشبكات الإنترنت والبيانات المخزنة والمتداولة عبرها[١].

**الردع السيبراني:** الردع أصلاً في العلاقات الصراعية الدولية هو «توفر القدرة على إرغام الخصم على التراجع عن تصرف معين أو إحباط الأهداف التي يتوخّاها من هذا التصرف، وذلك التراجع يأتي تحت التهديد بإلحاق خسارة جسيمة به تفوق المزايا التي يتوقعها من جراء تصرّفه هذا»[٢]. وعادة تستخدم القوى الكبرى «الردع» لمنع هجمات أعدائها عليها وتكبيدها خسائر أو جرها إلى حروب لا ترغبها، وعندما دخلت الحروب والهجمات السيبرانية حيّز الواقع الدولي، فقد فرض مفهوم «الردع» نفسه في المجال السيبراني كي يقلل من العدوانية السيبرانية – إن جاز التعبير – للقوى المختلفة، ووجدنا رئيس الولايات المتحدة الحالي جو بايدن يهدّد روسيا الاتحادية برد قوي على أي هجمات سيبرانية تشنّها ضد الولايات المتحدة قائلاً لرئيس روسيا الاتحادية: «إننا سننتقم وسنرد بالمثل»[٣]. وطبعاً فإن هذا يدخل في إطار «الردع السيبراني». لكن هناك مشكلات تكتنف مثل هذا الردع، ومنها صعوبة اكتشاف الجهة التي أطلقت هجوماً سيبرانياً «ما» أصلاً، وسهولة إنكار الجهة المهاجمة بسبب صعوبة إثبات التهمة عليها. ومن هذه المشكلات أيضاً: سهولة تأجير الدول والجهات المختلفة لهاكرز محترفين مستقلين عن أي دولة وإغرائهم بالمال لشنّ هجمات سيبرانية على دول أخرى لتحقيق أهداف سياسية.

**ولهذه الحرب السيبرانية الباردة وسائل عدة، منها: الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وحرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية.**

(١) انظر: صلاح حيدر عبد الواحد، م.س.ذ، ص ٦٥ وما بعدها.

(٢) انظر: إسماعيل صبري مقلد، الاستراتيجية والسياسة الدولية.. المفاهيم والحقائق الأساسية، ط مؤسسة الأبحاث العربية، بيروت ١٩٨٥، الطبعة الثانية، ص ١٨١.

(٣) انظر: أحمد عبد الحكيم، هل تعيد «الهجمات السيبرانية» بين الدول الكبرى أجواء الحرب الباردة، على موقع إندبندنت عربية، بتاريخ ١٠ يوليو ٢٠٢١، على الرابط التالي: https://cutt.us/UrPwe، تاريخ المشاهدة ٢٥ مايو ٢٠٢٢.

**الدفاع السيبراني:** فرضت المخاطر السيبرانية المعاصرة أن يكون للدول الكبرى والمتوسطة وللشركات الكبرى خطط وترتيبات لتحقيق دفاع مناسب لمصالحها وممتلكاتها ضد الهجمات السيبرانية أياً كان مصدرها، وصارت هذه القوى تنفق أموالاً وتخصّص فرقاً متخصّصة وتقنيات مناسبة للحماية المسبقة ضد أي هجمات سيبرانية أياً كان مصدرها. وتتلخّص الأساليب التقنية للدفاع ضد الهجمات السيبرانية في عدد من الإجراءات والأساليب، أبرزها[1]:

- استعمال الجدران النارية (Firwall).

- استخدام البرامج المضادة للبرمجيات الخبيثة أو الفيروسات (Antivirus Program).

- استخدام أنظمة كشف التسلل (IDS).

- فصل وتقسيم الشبكات.

- التشديد على بيانات الدخول.

- إجراء عمل النسخ الاحتياطي (Backup).

وعلى سبيل المثال[2]: فقد طورت القيادة الإلكترونية الأمريكية استراتيجية في عام ٢٠١٨ أطلقت عليها «المشاركة المستمرة» لمواجهة المنافسين الذين «يعملون باستمرار دون عتبة الصراع المسلح لإضعاف المؤسسات واكتساب مزايا استراتيجية». وهدف هذه الاستراتيجية هو «حرمان الأعداء من فرصة اختراق الأنظمة الأمريكية على مستوى العالم».

**السلاح السيبراني:** ويقصد به ترسانة السلاح الرقمي، أي الأدوات التقنية والبرامج الرقمية اللازمة لشنّ حرب سيبرانية احترافية، وليس من قبيل ما يفعله الهواة من استخدام برامج وأدوات متاحة للجميع بشكل عام؛ فالدول الكبرى تبني ترسانة سلاح رقمي سرية وتجربها باستمرار لتكون جاهزة للاستخدام ضد أهداف خصومها، وعلى سبيل المثال: خصصت روسيا الاتحادية ١٣٠ مليون دولار سنوياً لهذا الغرض، وتشمل ترسانتها شبكات ضخمة من البوتات Bots منتشرة في العديد من البلدان تستطيع استخدامها لشن هجوم تعطيل المواقع Sits أو التجسس السيبراني، كما تشمل ترسانتها أسلحة كهرومغناطيسية يمكنها تعطيل المعدات وأجهزة الاتصال والشبكات Networks، كما تمتلك برامج مزيفة تحتوي على فيروسات انتشار ذاتي، وكذا أنظمة متقدمة للكشف عن الثغرات في مواقع العدو الإلكترونية وتوظيفها، بجانب قنابل رقمية تنتظر الأوامر من أجل تخريب البنى التحتية الإلكترونية للعدو[3]) ولا شك في أن الولايات المتحدة وأوروبا الغربية تمتلك أنظمة كهذه وأكثر تطوراً منها، باعتبار أن الولايات المتحدة هي الدولة الأولى في العالم من حيث التقدم التقني في مجال الإنترنت والذكاء

---

(١) انظر: صلاح حيدر عبد الواحد، م.س.ذ، ص ٥٨ وما بعدها.

(٢) برس يوراس كرمانو وآخرون، تريبواير لحرب حقيقية؟ قواعد الاشتباك الغامضة السيبرانية، جريدة الخليج جازيت، ١٥ فبراير ٢٠٢٢، على الرابط التالي: https://cutt.us/25CYl، تاريخ المشاهدة ٢٥ مايو ٢٠٢٢.

(٣) انظر: عباس بدران، الحرب الإلكترونية الاشتباك في عالم المعلومات، ط مركز دراسات الحكومة الإلكترونية، بيروت ٢٠١٠، ص ٤٥-٤٦.

الصناعي، وقد استخدمت ذلك كله مراراً بدرجات متفاوتة ضد العراق ويوغسلافيا وإيران، وكانت القيادة السيبرانية الأمريكية قد خططت لشن هجوم سيبراني استراتيجي على إيران، حيث أعلنت هذه الخطة في ٢٠١٦، وعرفت هذه العملية باسم «نيترو زيوس» (Nitro Zeus)، وهي خطة مفصلة لشنّ هجوم سيبراني على إيران في حالة فشل الجهود الدبلوماسية للحدّ من برنامجها النووي واندلاع صراع عسكري، وكانت الخطة مصممة لتعطيل شبكة الدفاع الجوي الإيرانية، ونظم الاتصالات، والأجزاء الحساسة من شبكة الطاقة، وقد تم التراجع عن الخطة في يوليو ٢٠١٥ بعد إبرام الاتفاق النووي بين إيران والدول الست الكبرى. ويعتقد أن التخطيط لعملية «نيترو زيوس» قد استغرق سنوات من الإعداد والاستطلاع والمحاكاة واختبار البرامج الضارة[١].

**بنك الأهداف في الحرب السيبرانية:** الحرب السيبرانية مثلها مثل الحرب العسكرية الساخنة تحتاج لتحديد بنك أهداف كي تستهدفها بأسلحتها، وهو ما يفرض وجود عمليات استطلاع لتحديد هذه الأهداف السيبرانية ونقاط ضعفها وسبل استهدافها وفق كل السيناريوهات المتوقعة، إن في هجمات سيبرانية محدودة أو شاملة، وسواء كانت سيبرانية منفردة أم سيبرانية متواكبة مع حرب عسكرية ساخنة[٢].

**قواعد الاشتباك السيبراني:** في الحروب العسكرية المعتادة هناك العديد من القوانين والاتفاقات الدولية التي تضع أطراً وقواعد متعددة لمثل هذه الاشتباكات العسكرية وما ينتج عنها أو يترتب عليها من أعمال أو واقع أو وقائع، لكن الأمر في الهجمات والحروب السيبرانية مختلف، فلا توجد معاهدات للحدّ من الأسلحة تقضي بمنع القرصنة المدعومة من الدولة، والتي غالباً ما تكون محمية بالإنكار المعقول؛ لأنه غالباً ما يصعب تحديد هوية المهاجمين بالسرعة الكافية. وفي عام ٢٠١٥ اتفقت القوى الكبرى وغيرها في الأمم المتحدة على مجموعة من ١١ معياراً طوعياً للسلوك السيبراني الدولي، لكن منذئذ يجري تجاهل هذه المعايير باستمرار، كما أن المخالفين ليسوا عرضة للمساءلة في الأمم المتحدة بأي حال من الأحوال[٣].

**تستخدم القوى الدولية الكبرى حالياً الفضاء الإلكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة أولى لحواسيب العدو، واختراق العمليات العسكرية للخصوم سيبرانيّاً، أو حتى استهداف الحياة المدنية، والبنية التحتية المعلوماتية.**

---

(١) انظر: شادي عبد الوهاب، السيناريو الكارثي متى تتحول الحرب السيبرانية إلى حرب شاملة، بحث على موقع مركز المستقبل للأبحاث والدراسات المتقدمة، على الرابط التالي: https://cutt.us/BuJnY، تاريخ المشاهدة ٢٧ مايو ٢٠٢٢.

(٢) عباس بدران، م.س.ذ، ص ٤٢ وما بعدها.

(٣) برس يوراس كرمانو وآخرون، تريبواير لحرب حقيقية؟ قواعد الاشتباك الغامضة

ورغم أن العديد من مؤسسات وفاعليات منظمة الأمم المتحدة[1] قد أصدرت العديد من البيانات والتقارير وعقدت مؤتمرات وورشاً بحثية وأصدرت أدلة تعامل منذ ١٩٩٤ حتى اليوم، وقد انصبت كلها على تعريف وتجريم الهجمات السيبرانية، وحضت الدول على التعاون معها في ذلك؛ إلا أن ذلك كله لم يرسخ قواعد وقوانين محددة وواضحة وملزمة تنظم قواعد الاشتباك في الفضاء السيبراني على مستوى العالم، ولذلك كله يرى أحد الباحثين – محقاً – أن «التكييف القانوني للهجمات الإلكترونية لم يصل بعد إلى مرحلة إبرام اتفاقيات دولية صريحة، وبحيث تكون متعددة الأطراف، وتنظم الهجمات الإلكترونية وفق نصوص وقواعد قانونية صريحة، وهو ما يُعزى إلى أسباب عدة، يأتي في مقدمتها وجود عقبات تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني، مثل الولايات المتحدة الأمريكية، وروسيا، والصين، إذ إن هذه الدول لا تفضّل طرح موضوع التنظيم على المنابر الدولية حتى لا تفقد موقعها المهم بين الدول المهيمنة، وهو ما يضرّ بأمنها القومي. يضاف إلى ذلك أن بقاء الموضوع خارج حدود القضايا القانونية يتيح لهذه الدول مساحة واسعة لكي تتحرك في توظيف أسلحتها الإلكترونية لتحقيق أهدافها، ومع ذلك تبقى خارج نطاق المساءلة القانونية»[2].

وبجانب ذلك تواصلت الهجمات السيبرانية بأنواعها المختلفة في شتى أنحاء العالم، خاصة من قوى كبرى خاصة روسيا والصين والولايات المتحدة.

**فرضت المخاطر السيبرانية المعاصرة أن يكون للدول الكبرى والمتوسطة وللشركات الكبرى خطط وترتيبات لتحقيق دفاع مناسب لمصالحها وممتلكاتها ضد الهجمات السيبرانية أياً كان مصدرها.**

**الجريمة السيبرانية:**
هذا المفهوم أو المصطلح هو من أوائل المفاهيم التي تداولها الفكر السياسي والقانوني في العالم مع بدايات انتشار الحواسيب وبداية نشأة الشبكات التي تربط الحواسيب. وقد اهتمت الدول والمنظمات الدولية كالأمم المتحدة وغيرها بتعريف «الجريمة السيبرانية» باعتبارها تشمل طائفة واسعة من الجرائم المرتكبة بدافع مالي، والجرائم المتصلة بالمحتوى الحاسوبي، فضلاً عن الأعمال التي تمسّ بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها بغرض إجرامي[3].

**الإرهاب السيبراني:** مصطلح الإرهاب ما زال مصطلحاً عائماً لم يجرِ أي اتفاق دولي عام على تحديد مدلول جامع مانع له، ومن

---

السيبرانية، م.س.ذ.

(١) انظر عرضاً ضافياً لكل هذه الاتفاقات الدولية والإقليمية في: صلاح حيدر عبد الواحد، م.س.ذ، ص ٦٤ وما بعدها.

(٢) نفس المرجع، ص ٥٣.

(٣) مكتب الأمم المتحدة المعني بالمخدرات والجرائم، دراسة شاملة عن الجريمة السيبرانية، مسودة، نيويورك ٢٠١٣، ص (xiv) وما بعدها.

هنا فإن مفهوم الإرهاب السيبراني سيظل يدور في نفس الفلك العائم، وسيظل مصطلح «الإرهاب السيبراني» مطروحاً للأخذ والرد، كما أن الأطراف المتصارعة سيبرانيّاً والمتعادية سياسياً أو عقيدياً ستظل تتهم بعضها البعض بتهمة الإرهاب السيبراني، رغم أنه لم تجرِ بعد عمليات تخريب أو تدمير شامل أو إزهاق أرواح عبر هجمات سيبرانية حتى كتابة هذه السطور، وتظل الاتهامات في هذا المجال محصورة في مجال التجنيد أو التعبئة أو التحريض لأغراض عمليات إرهابية.

**الجيش السيبراني:** ويعبر عنه بعض الباحثين بـ «القوة الرابعة»، باعتبار أن الجيش جوي وبري وبحري بينما الجيش السيبراني هو الرابع، وقد أنشأت كل القوى الكبرى في العالم إدارات متخصصة لهذا الغرض، وعلى سبيل المثال لا الحصر ففي الولايات المتحدة نجد أن وزارة الدفاع مسؤولة عن الدفاع والهجوم السيبراني في المجال العسكري وعن تقديم المساعدة للجهات المدنية في نفس المجال، ولهذا الغرض أنشئت القيادة السيبرانية للولايات المتحدة (United States Cyber Command) بوصفها جزءاً من القيادة الاستراتيجية في وزارة الدفاع، ونجد إدارات مناظرة أو مشابهة في بقية الدول الكبرى[1].

استخدامات وأهداف الحرب السيبرانية

من الملاحظ أن للهجمات السيبرانية العديد من الأهداف المختلفة، **فمنها: الضغط على الخصم في إطار صراع محدد معه**، ومن أمثلة ذلك هجوم إلكتروني وقع في ٢٦ أكتوبر ٢٠٢١ على نظام توزيع الوقود في إيران أدى إلى شلل محطات الوقود في البلاد البالغ عددها ٤٣٠٠ محطة، والتي استغرقت ١٢ يوماً لاستعادة الخدمة بالكامل، وهو ما ردت عليه إيران بشنّ هجوم سيبراني على منشأة طبية إسرائيلية كبرى[2].

**كما كان منها ما استهدف التحكم في مجريات الأحداث داخل دولة الخصم**، والأمثلة الأبرز في ذلك هو الهجمات السيبرانية التي مثّلت تدخلات روسيا الاتحادية في الانتخابات الأمريكية بهدف ترجيح كفة دونالد ترامب في الانتخابات الرئاسية الأمريكية أثناء خوضه الانتخابات الرئاسية في مواجهة هيلاري كلينتون في ٢٠١٦، وكذلك تدخّلات كلٍّ من روسيا وإيران والصين في الانتخابات الرئاسية الأمريكية الأخيرة بين بايدن وترامب، والتي حاولت فيها روسيا الاتحادية ترجيح كفة ترامب على بايدن[3].

---

(١) حول مزيد من التفاصيل عن إدارات الحرب السيبرانية في الدول الكبرى في العالم، راجع: بدون مؤلف، حرب التحكم الآلي سلاح الحرب الخامس، دار الجليل، الطبعة الأولى، عَمَّان ٢٠١٣، ص ٦٥ وما بعدها.

(٢) انظر: شادي عبدالوهاب، م.س.ذ.

(٣) أورد موقع **ccn** الخبر التالي (١٦ مارس ٢٠٢١): نشر مكتب مدير الاستخبارات الوطنية تقريره حول التهديدات الخارجية لانتخابات الرئاسة الأمريكية الأخيرة، وكشف عن أن قوى خارجية، من ضمنها روسيا، حاولت التأثير على سير الانتخابات، وكان هدفها تشويه سمعة حملة الرئيس جو بايدن والحزب الديمقراطي، ودعم الرئيس السابق دونالد ترامب، مقوضة ثقة الرأي العام في العملية الانتخابية وتغذية الانقسامات الاجتماعية في الولايات المتحدة. وقال التقرير: على عكس ما جرى في انتخابات ٢٠١٦، لم نر جهوداً سيبرانية روسية للوصول إلى قاعدة البيانات الخاصة بالانتخابات. وكشف التقرير: إن إيران والصين بذلتا جهوداً للتدخل بالانتخابات الرئاسية الأمريكية، وإن طهران حاولت تشويه حملة ترامب الانتخابية دون دعم منافسه (جو بايدن)، لكنه أكد أن بكين لم تبذل جهوداً مباشرة لتغيير نتائج الانتخابات. نقلاً عن تقرير إخباري

ومــن ذلك أيضــاً التدخــلات الســيبرانية الروســية فــي بريطانيــا للتأثيــر فــي الناخب البريطانــي لإعطــاء دفعــة قوية لاتجــاه خروج بريطانيا من الاتحاد الأوروبي[1].

**وهناك نوع ثالث من الهجمات استهدف سرقة المعلومات** التقنية أو الاقتصادية أو العسكرية أو حتى السياســية، وأبرزها مــا تقــوم بــه الصــين وروســيا الاتحادية وكوريا الشــمالية تجاه الولايات المتحــدة، وبعضهــا تجاه أوروبا، كما تقوم الولايات المتحدة بذلك تجاه العالم كلــه، وأيضاً تقــوم القوى الأوروبية بالعديد من هذه الأنشطة[2].

**الأمثلــة الأبــرز فــي ذلــك هــو الهجمات الســيبرانية التي مثّلت تدخــلات روســيا الاتحاديــة فــي الانتخابات الأمريكية بهدف ترجيح كفة دونالد ترامب في الانتخابات الرئاســية الأمريكية أثنــاء خوضه الانتخابات الرئاســية في مواجهة هيلاري كلينتون في ٢٠١٦**

**أمــا النــوع الرابــع مــن الهجمــات الســيبرانية** فهو ما يســتهدف سرقة أموال أو الحصول على أموال عبر ما يســمى بصيغــة الفدية، حيث يتم اختراق نظام تشــغيل ما أو شــبكة مــا وتعطيل عمل الشــركة أو الشــبكة أو المؤسســة أو المنشأة حتى يتم دفع الفدية المطلوبة، أو اختراق أنظمة مالية وتحويــل الأموال منها إلــى الهاكرز الذي ينفــذ الهجوم، ومن أمثلة الهجمات الســيبرانية للحصــول علــى الأموال: عملية ســرقة عملات مشــفرة بقيمة ٦٠٠ مليون دولار التي وقعت في مــارس الماضي وأعلنت عنهــا الـ FBI، كما قام مجرمو الإنترنت الكوريون الشماليون بسرقة أكثر من ٤٠٠ مليون دولار عام ٢٠٢١ وحــده[3]. ويتوقــع أن تبلغ خسائر الهجمات السيبرانية ١٠,٥ تريليون دولار سنوياً بدءاً من عام ٢٠٢٥ ببرامــج الفديــة - أو غيرهــا، وذلك مقارنة بـــ ٣ تريليونات فقط في عام ٢٠١٥، وهــذا الرقم أكبر مــن أضرار الكوارث الطبيعية الســنوية، كما أنه أكبر من أرباح تجارة المخدرات في العالم[4].

**وهنــاك نــوع خامــس**، وهــو الهجمــات التي يقــوم بهــا - أو من الممكن أن يقــوم بها - أفراد أو منظمــات ليســت حكوميــة، مثــل المنظمات الإرهابيــة أو حــركات المقاومة ضــد الاحتلال، وهــي التــي اقترحها وأفســح لها إميــل خوري المجــال فــي صفحــات كتابــه وكأنه يدعــو لها لضرب أو الضغط على ما يسميه الإمبراطورية

بعنوان «تقرير للاستخبارات الأمريكية: روسيا وإيران تدخلتا في الانتخابات الرئاسية ٢٠٢٠»، بتاريخ ١٦ مارس ٢٠٢١، على الرابط التالي: **https://cutt.us/b2oZ3**، تاريخ المشاهدة ٢٧ مايو ٢٠٢٢.

(١) للاطلاع على تقارير إخبارية عن هذا الموضوع يمكنك الرجوع لكل من الرابطين التاليين: **https://cutt.us/iue94**.. و**https://cutt.us/FsvCX**، تاريخ المشاهدة ٢٧ مايو ٢٠٢٢.

(٢) سرقة كل من الصين وروسيا الاتحادية وكوريا الشمالية المعلومات عبر تجسس سيبراني من كل من الولايات المتحدة وأوروبا، وكذلك التجسس السيبراني من قبل الولايات المتحدة على العالم كله أمر مشهور ومنتشر جداً في سائر مصادر الأخبار، وانظر على سبيل المثال لا الحصر: **https://cutt.us/tyv36** حول التجسس الصيني على الولايات المتحدة، وأيضاً: **https://cutt.us/4XbA4**، وحول التجسس السيبراني الأمريكي على كبار قادة الدول الأوروبية انظر تقريراً على الرابط التالي: **https://cutt.us/dPeZ3**.

(٣) انظر الخبر على الرابط التالي: **https://2u.pw/i6tAm**، تاريخ المشاهدة ١٧ أبريل ٢٠٢٢.

(٤) انظر تقريراً على الرابط التالي: **https://cutt.us/fNxyx**، تاريخ المشاهدة ١٧ أبريل ٢٠٢٢.

الأمريكية[١]، ويمكننا اعتبار أن من أمثلة هذا النوع من الحروب السيبرانية ما حدث مؤخراً من اختراق مجهولين لملفات الشرطة الصينية وفضح عمليات السجن والتعذيب للأقلية المسلمة من الإيغور الصينيين، وجاء التسريب بالتزامن مع زيارة المفوضة الأممية لحقوق الإنسان «ميشيل باشليت» للصين كي يحرج الأخيرة بأشد ما يمكن[٢].

لكن يبدو أن هذا النوع الخامس لم يتم التوسع فيه حتى الآن وفق متابعتنا في هذه السنوات الأخيرة حتى كتابة هذا البحث.

**وأخيراً لاحظنا أسلوباً آخر من الحرب السيبرانية** دار في الحرب الروسية - الأوكرانية الدائرة الآن (النصف الأول من عام ٢٠٢٢)، فعلى الرغم من أنها حرب عسكرية تقليدية ساخنة، إلا أن الهجمات السيبرانية استخدمت فيها؛ فروسيا شنّت هجومها السيبراني قبل يوم واحد من غزوها لأوكرانيا فأصاب الشلل مواقع حكومية مهمة، ومنها مقار الحكومة والبرلمان ووزارة الخارجية ومؤسسات عديدة.

واستخدم هذا الهجوم أسلوب (DDos)، أي الحرمان من الخدمة، عبر إغراق الخوادم بطلبات كثيفة غير مشروعة، ما يحمّل البنية التحتية للخوادم أكثر من قدرتها، ويؤدي إلى توقّفها عن العمل، كما تم العثور على برامج تسمى (Wiper) وهي برامج ضارة يمكنها حذف الكثير من البيانات دون ملاحظة ذلك، ما يسبب أضراراً اقتصادية ضخمة. وجاء رد أوكرانيا السيبراني على روسيا عندما تطوعت مجموعة قراصنة (Anonymous) التي أعلنت الحرب السيبرانية على روسيا، ما أدى إلى تعطيل العديد من المواقع الحكومية في روسيا، كما تعرض للهجوم السيبراني موقع قناة rt.com التي يعتبرها الغرب أداة بروبوغاندا للكرملين[٣].

## مسار الحروب السيبرانية

الإنسان هو الإنسان، سواء كان في الواقع الفعلي على الأرض أو كان في الواقع الافتراضي أي السيبراني بواسطة شبكة الإنترنت والتطبيقات الرقمية وأجهزة الحاسوب وإنترنت الأشياء؛ فرغبات الإنسان ونزعاته إن في الخير والعدل أو في الشهوات والمال أو التسلية واللهو أو العدوان على الآخرين؛ هي نفسها، فهي سواء إن في الواقع العملي على الأرض أو في الواقع الافتراضي عبر الفضاء السيبراني. ومن هنا نجد أن كل هذه النوازع والرغبات تنتشر في الواقع السيبراني، وسيزداد

---

(١) انظر على سبيل المثال لا الحصر، إميل خوري، م.س.ذ، ص ٢٥٦ وما بعدها، وأيضاً ص ٢٦٩ وما بعدها.

(٢) تم تسريب «ملفات شرطة شينجيانغ» التي تتضمن الآلاف من الوثائق والصور والخطابات الرسمية عن معسكرات تحتجز أفراداً من أقلية الإيغور المسلمة من قبل مصدر مجهول إلى عالم الأنثروبولوجيا الألماني أدريان تسنتس، الذي يعمل في مؤسسة النصب التذكاري لضحايا الشيوعية في واشنطن، وهذه الملفات جاءت بالطبع عبر اختراق أنظمة كمبيوتر في مكتب الأمن العام في مقاطعتي إيلي وكاشغر في منطقة شينجيانغ، والشخص الذي لا يريد التعريف بنفسه بسبب دواع أمنية، زوده بالبيانات دون أي شروط ولا دفع أي أموال، ومن ثم نقلها الباحثُ الألماني إلى وسائل الإعلام، وهذه التسريبات تفضح الكذب الصيني حول هذه المعسكرات وما يجري فيها، وتدعم الاتهامات للصين بممارسة إبادة ضد المسلمين في الصين، انظر مزيداً من التفاصيل على الرابط التالي: **https://cutt.us/mJMrM** تاريخ المشاهدة ٢٧ مايو ٢٠٢٢.

(٣) موقع دويتش فيله، الحرب في أوكرانيا أي دور تلعبه الهجمات السيبرانية، على الرابط التالي: **https://cutt.us/6MqEl**، تاريخ المشاهدة ٢٨ مايو ٢٠٢٢.

وجودها كلما زادت قدرة الإنسان على استخدام هذا الفضاء السيبراني، وفي قلب ذلك كله يأتي الصراع والحرب والهجمات السيبرانية المتعددة بكل أنواعها، ولا يظن أحد أن التقدم العلمي قد يقيّد رغبات ونوازع الإنسان أو يغلب عليها طابع العقل والمنطق، فالأمر كما قال كلاوزفيتز عن طبيعة الحرب: «من الممكن أن يجرف الحقد الشرس أكثر الأمم تمدّناً وتحضراً»[1]. ونعتبر أنه يمكننا تعميم مقولته هذه فلا تظل منحصرة في مجال الحقد والعدوانية، بل تمتد لكافة رغبات البشر وشهواتهم في المجالات كافة.

ونظراً لأن الصراع أعمّ من الحرب، فإن الحرب السيبرانية تأتي كأداة مهمة في أي صراع دولي أو إقليمي أو محلي في المرحلة الحالية، وستزداد أهميتها كلما مرّ الوقت بسبب التحول الرقمي والتقدم الرقمي والسهولة في حيازة التقنيات اللازمة لشنّ الهجمات السيبرانية أياً كان هدفها، بجانب ازدياد تحول التطبيقات الرقمية والحوسبة والإنترنت وكذلك إنترنت الأشياء إلى العصب الأساسي لكل موقع أو منشأة أو ماكينة أو آلة مدنية كانت أو عسكرية، سواء كانت تعمل في البر أو في البحر أو في الجو أو حتى في الفضاء الخارجي، ومن ثم صارت كلها عصب الدولة المعاصرة أيا كانت طبيعة النظام الدولي، وبالتالي فالهجوم على هذا العصب وشله أو إيذاؤه سيمثّل مكسباً للخصوم وخسارة للجهة المستهدفة.

**الحرب السيبرانية تأتي كأداة مهمة في أي صراع دولي أو إقليمي أو محلي في المرحلة الحالية، وستزداد أهميتها كلما مرّ الوقت بسبب التحول الرقمي والتقدم الرقمي والسهولة في حيازة التقنيات اللازمة لشنّ الهجمات السيبرانية أياً كان هدفها.**

ونظراً لأن القدرة على الهجوم السيبراني وإيقاع الضرر عبر الهجمات السيبرانية صار أمراً مقدوراً لأحاد الناس من الأفراد والمجموعات الصغيرة؛ فإن شنّ الحرب أو التهديد السيبراني ليس حكراً على الدول، لكنه مقدور لكل من حاز علماً كافياً بالحوسبة والبرمجة الحاسوبية والإنترنت وما يتعلق بها، ولا يحتاج إلى مال كثير ولا أدوات كثيرة.

ومن هنا، فإن القدرة على شنّ الحروب والهجمات السيبرانية تشجّع على إلهاب الصراع الدولي وتغذي العدوانية عند العديد من القوى الدولية والإقليمية والمجموعات غير الحكومية. وقد تُسحب القوى المتصارعة للانزلاق إلى حرب باردة أو حرب ساخنة تقليدية، كما أنها قد تصير إحدى أدوات الحرب الباردة أو الحرب الساخنة، سواء كانت حرباً عسكرية تقليدية أو حرباً هجينة من قبيل حروب الجيل الرابع.

ومن جهة ثانية، سيؤدي هذا كله لزيادة

---

(١) انظر: الوجيز في الحرب، م.س.ذ، ص ٧٦.

إنفاق الدول والكيانات – من شركات وهيئات ومنظمات - جهداً ومالاً وتقنيات على عملية الدفاع والأمن السيبراني، فضلاً عن اتجاه القوى الكبرى (دول وكيانات) للتجهّز للوصول للقدرة على الردع السيبراني.

وأخيراً، ستمثّل عملية وأدوات الحروب والهجمات السيبرانية فرصة للمستضعفين والمظلومين للانتصاف بدرجة أو أخرى من ظالميهم ومستضعفيهم عبر استخدام الهجمات والحروب السيبرانية بسبب انخفاض تكلفتها والسهولة النسبية لاستخدامها وفرص الإفلات منها دون خسائر أو بخسائر محدودة، كما رأينا في الهجمة السيبرانية الأخيرة على الصين التي نتج عنها أخذ نسخة من مستندات الشرطة الصينية في مكان احتجاز وتعذيب الملايين من أقلية الإيغور الصينية المسلمة ونشرها على الرأي العام العالمي وفضح جمهورية الصين، ما تسبب في الضغط عليها سياسياً ومعنوياً، كما أشرنا في الصفحات السابقة. كما أنها تشكّل ثغرة واسعة أمام كل ناعق يريد أن يهدّد أمن دولنا، خاصة أننا أمام تلك الهجمات الإلكترونية لا نمتلك التكنولوجيا المتقدمة التي تتيح لنا صدّ هكذا هجمات، أو مواجهاتها، وأصبحنا في حالة دافعة دائمة بوسائل ضعيفة.

## مستقبل الحروب السيبرانية والصراع بين الدول

كي نفهم دور الحروب السيبرانية وأثرها في الصراع الدولي المعاصر، لا بد من أن نضعها في سياق الحروب المعتادة، سواء الحروب الباردة أو الساخنة؛ فهذه الحروب مجرد أساليب يجري من خلالها الصراع الذي اعتاد عليه البشر عبر تاريخ البشرية منذ بداية خلق الإنسان، فكلما تعارضت مصالح ورغبات البشر أو تنافست تنافساً يصل للخصومة، حينئذ تندلع الحرب أو الصراع بين القوى أو الدول، ويأخذ هذا الصراع عادة الشكل الساخن أو البارد. وكما أوضحنا في الصفحات السابقة، فإن غاية الحرب هي إخضاع إرادة الخصم أو تليين إرادة هذا الخصم للحصول على عدد من التنازلات منه حول الموضوع محل الصراع أو محل التنافس. واعتاد البشر منذ نشأة الدول في أقدم العصور وحتى اليوم، على استخدام كل الأدوات والأسلحة والأساليب التي تتاح لهم في حروبهم وصراعاتهم، وباستمرار سخّروا الفكر والبحوث العلمية والصناعة والتكنولوجيا والاقتصاد وحتى الطب والدواء وكل شيء؛ لإحداث التطوير في أدوات وأساليب وأسلحة الصراع، وكلما ابتكروا سلاحاً أو أداة أو أسلوباً أو فكراً، سارعوا إلى توظيفه في صراعاتهم لتحقيق غاياتهم الصراعية. وفي هذا السياق يمكن فهم الدور الذي تلعبه وستلعبه الحرب السيبرانية في الصراع الدولي، سواء على المدى القريب أو في المستقبل أيضاً، حيث سيتم توظيفها في الصراعات بأقصى ما يستطيع كل طرف من أطراف الصراع.

لكن لا بد من ملاحظة أنه منذ نهاية الحرب العالمية الثانية فإن الحرب الساخنة أو الباردة التقليدية وغير التقليدية قد وضعوا

لها قواعد (سـواء قانونية أو سياسـية عرفية) كي لا تنزلق لحالة لا يمكن السـيطرة فيها على مداهـا الجغرافـي والتدميري، والتزمـوا بهذه القواعـد لحدّ كبير جداً منذئـذ حتى الآن، كما ابتكروا أسـاليب واسـتراتيجيات للحرب تحقق لهم أهدافهـم أو قدراً منها دون الانزلاق لحرب عالميـة شـاملة أو عظمى، كاسـتراتيجية حافة الهاويـة أو الحـرب بالوكالة أو الحـرب الباردة أو الأحلاف العسكرية أو الردع... إلخ. وباعتبار أن التاريـخ يشـير لتوجهات المسـتقبل، فالمتوقـع أن القـوى المتحكّمـة فـي النظام الدولي سـتحاول جعل الحـروب والهجمات السـيبرانية لا تخـرج عـن إطار تحدده يسـمح بممارسـة الصـراع دون خروجـه عـن الضوابـط التي رسـختها للصراع الدولي المعاصر في إطار النظـام الدولـي القائـم. وحتى في حالـة تغيّر النظـام الدولـي، فـإن النظام الدولـي الجديد سيسـير على نفس فكرة تقنـين الصراع الدولي أياً كانت أدواته، سـواء حرباً عسكرية ساخنة أو حرباً باردة أو حرباً سيبرانية، لكن السؤال هو:

**القـدرة علـى شـنّ الحـروب والهجمـات السـيبرانية تشـجّع علـى إلهاب الصراع الدولي وتغذي العدوانيـة عند العديـد من القوى الدولية والإقليميـة والمجموعات غير الحكومية. وقد تُسحب القوى المتصارعـة للانزلاق إلى حرب باردة أو حرب ساخنة.**

هل سـيلتزم جميـع الفاعلين فـي الفضاء السيبراني بعملية تقنين الصراع السيبراني على هذا النحو الذي سـتحدده القـوى المهيمنة على النظـام الدولي؟ أم أن سـهولة وانخفاض تكلفة شنّ هجمات سيبرانية كبرى سيحفز العديد من اللاعبـين المتمرديـن على النظـام الدولي لمزيد مـن الاشـتباك السـيبراني دون أن يعبـؤوا بما تضعه القوى الكبرى من قواعد وضوابط لتقنين الصراع السيبراني؟

ولـو حـدث هـذا التمـرد فهنـاك ثلاثـة سيناريوهات متوقعة، هي:

- يتمكـن المتمـردون مـن تغيير قواعد الصراع والاشـتباك السـيبراني وفقـاً لأهدافهم، وينصاع لهـم النظـام الدولـي، وسيشـكل ذلـك نوعـاً مـن التغييـر فـي النظام الدولي.

- تقرر قـوى النظام الدولي سـحق المتمردين وتنجـح فـي ذلك، مـا يرسـخ النظـام الدولي وقوانينه بشأن الصراع والاشتباك السيبراني.

- لا ينجـح المتمردون في إقـرار قواعدهم للصراع والاشـتباك السـيبراني، كمـا لا ينجح النظـام الدولي في إلزامهـم بقواعده، ويظل كلٌّ مـن الطرفـين مصممـاً على مسـلكه، ما يخلق فوضى في مجال الصراع والهجمات السيبرانية وربما في الصراع الدولي نفسه بشكل عام، لكن هذا الحال قد يستمر لمدى زمني قصير، ثم على المدى الزمني المتوسط أو البعيد، سيصاب سائر الأطراف بشـيء مـن الإنهاك يدفعهـم للتفاهم

لتحقيق إما السيناريو الأول أو الثاني.

وهذا استشـراف عـام بشـأن مجمل آفاق اسـتخدام الهجمـات والحـروب السـيبرانية باعتبارهـا أمـراً لـم تسـتقر قواعـد وقوانين وأعـراف ممارسـته ضمـن الصـراع الدولـي المعاصر، لكن هناك أسئلة أخرى جديرة بالتفكر حول إجاباتها، وهي:

هل سـتهدئ الحروب السـيبرانية الصراع الدولي أم ستزيده اشتعالاً؟ وهل ستؤدي الهجمات السيبرانية إلى اشتعال حروب عسكرية ساخنة، أم أنها سـتجعل الأطـراف تقنع بما حققته ضد أعدائها من خسائر وتكتفي بها فلا تلجأ للسلاح العسـكري التقليدي؟ وأيضاً هـل تتطور قدرات وتكتيكات الحرب السيبرانية فيمكن من خلالها تطويع إرادة الخصم ما يجعل الحرب السيبرانية بديلاً عن الحرب التقليدية؟

وكل الإجابات واردة؛ لأن الإنسـان هو أعقد شـيء على وجـه الأرض، فحيـازة القدرة تغري بالعـدوان وخوض الحروب، كمـا أن الردع يكف شـرور المعتدين، ومع ذلك فالحسابات الخاطئة مـن قائد أحمق أو أرعن أو متعصب قد تشـعل حرباً ساخنة[1] لا يعلم مداها وعواقبها لا مشعلها ولا المصطلي بنارها.

## الخاتمة

عـرض البحث لقضية الحـروب والهجمات السيبرانية وتعريفها وأدواتها وأساليبها وأهدافها وعلاقتها بالحروب العسكرية بأنواعها وأجيالها المختلفـة، وعلاقة ذلك كله بالصراعات الدولية، وأوضـح أنـواع وأنمـاط الهجمـات والحـروب السـيبرانية وكيفية تعامل القوى المختلفة معها، وآفـاق تطورها وتوظيفها في الصـراع الدولي. كما عرض لطبيعة الفاعلين في مجال الهجمات والحـروب السـيبرانية، وأوضـح العديـد مـن المفاهيم المتعلقة بالحروب السيبرانية، مثل:

الأمن السـيبراني، الردع السيبراني، الدفاع السيبراني، السلاح السيبراني، بنك الأهداف في الحرب السيبرانية، قواعد الاشتباك السيبراني، الجريمة السيبرانية، والإرهاب السيبراني.

وأشـار البحـث إلـى مـا تتيحـه الهجمات والحـروب السـيبرانية مـن فـرص وتفرضـه مـن مخاطر، كما عرض استشـرافاً لمساراتها المسـتقبلية، وتوقّع ما قد تصـل له من آفاق في مجال الصراع بين الدول، واستشـرف المستقبل في هذا الميدان، وأوضح السيناريوهات المتوقّعة في هذا الصدد.

---

(١) فضلاً عن حرب باردة أو سيبرانية.